IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Appellants:	Kammer et. al.
Title:	LOCATION BASED SECURITY MODIFICATION SYSTEM AND METHOD
Appl. No.:	10/053,013
Filing Date:	01/18/2002
Examiner:	Abedin, Shanto
Art Unit:	2131
Confirmation No.:	2103

CERTIFICATE OF EXPRESS MAILING
I hereby certify that this correspondence is being deposited with the United States Postal Service's "Express Mail Post Office To Addressee" service under 37 C.F.R. § 1.10 on the date indicated below and is addressed to: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

EV 962275132 US (Express Mail Label Number) — May 29, 2007 (Date of Deposit)

Deborah A. Kocorowski
(Printed Name)

Deborah A. Kocorowski
(Signature)

Mail Stop **APPEAL BRIEF - PATENTS**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Under the provisions of 37 C.F.R. § 41.37, this Appeal Brief is being filed together with a credit card payment form in the amount of $500.00 covering the 37 C.F.R. § 41.20(b)(2) appeal fee. If this fee is deemed to be insufficient, authorization is hereby given to charge any deficiency (or credit any balance) to the undersigned Deposit Account 19-0741.

REAL PARTY IN INTEREST

The real party in interest is Palm, Inc., of Sunnyvale, California.

05/31/2007 RFEKABU1 00000015 10053013
01 FC:1402 500.00 OP

RELATED APPEALS AND INTERFERENCES

There are no related appeals, interferences, or judicial proceedings known to the Appellants, the Appellants' legal representative, or assignee which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the present appeal.

STATUS OF CLAIMS

Claims 1-25 and 27-53 are currently rejected and are the subject of the present appeal. Claim 26 has been cancelled.

STATUS OF AMENDMENTS

Claims 1-25 and 27-53 were pending in the application when a final Office Action dated August 31, 2006 was issued. Appellants submitted an Amendment on December 5, 2006, which amended claim 30. In an Advisory Action dated January 4, 2007, the Examiner indicated that the Amendment submitted on December 5, 2006, would be entered, but that the Amendment did not place the application in condition for allowance. No amendments have been made since the date of the Advisory Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method of adjusting security for a network user node in communication with a network based upon the location of the node (p. 3, lines 21-27). The method includes determining the location of a network user node, (p. 8, lines 14-21; FIG. 2 (step 210)), selecting a single level of security from a group of more than two security levels based on the determined location (p. 9, lines 4-19; p. 10, lines 1-2), the group of more than two security levels being stored in the memory of the network user node, (p. 9 lines 7-11), and modifying the security protection for the network user node based upon the selected level of security, (p. 11, lines 4-6), wherein the group of more than two security levels is defined by a user of the network user node (p. 9, line 20 to p. 10, line 2).

Independent claim 18 is directed to a computer system for modifying security settings for a network user node based on the location of the node (p. 4, lines 1-13). The system includes an input device having a communicative coupling with a system for determining the location of a network user node, (p. 6, lines 23-27), a storage device for storing a table of security modifications to be performed based on a plurality of locations for the network user node, (p. 9, lines 7-11), the security modifications including more than two levels, (p. 10, lines 1-2), the security levels being defined by a user of the network user node, (p. 10, lines 10-18), a processor coupled to a storage device for processing information, storing on a storage device, and generating a security modification instruction, (p. 9, lines 11-12), and a communication device capable of transmitting a data signal to the network user node containing instructions to modify the security protection for the node (p. 10, line 27 to p. 11, line 2).

Independent claim 30 is directed to a method of adjusting security for a network user node having a processor, a memory coupled to the processor, a wireless transceiver, and a physical location determining device in communication with a network based upon the physical location of the node (p. 4, lines 14-21). The method includes receiving physical location information using a network user node, (p. 8, lines 14-21), and using a network user node to modify security protection for data to a single level from a group of more than two levels based upon the physical location information, wherein the group of more than two levels are defined by a user of the network user node (p. 9 line 20 to p. 10, line 9).

Independent claim 38 is directed to a system implemented on a network user node for modifying security settings based on the physical location of the node (p. 4 line 22 to p. 5 line 2). The system includes a system for determining the physical location of the network user node coupled to the network user node, (p. 8, lines 14-21), a processor for processing information, storing information on a storage device, and accessing a table of security modification instructions, (p. 9, lines 11-12), the table including more than two unique security modifications, (p. 10, lines 1-2), and a storage device coupled to the network user node for storing a table of security modifications, (p. 9, lines 7-11), wherein the network user

node performs security modifications based on the physical location of the network user node (p. 11, lines 4-6).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection presented for review are:

(1) Whether claims 1, 2-5, 7-9, 11-13, 15-16, 18, 19-21, 23-24, 27-28, 30, 31-36, 38, 39-41, 43-44, and 46-48 are unpatentable under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 6,970,927 ("Stewart et al.");

(2) Whether claims 6, 10, 14, 22, 25, 37, 42, and 45 are unpatentable under 35 U.S.C. § 103(a) over Stewart et al. in view of U.S. Patent Appl. Publ. No. 2002/0138632 ("Bade et al."); and

(3) Whether claims 17, 29, and 49 are unpatentable under 35 U.S.C. § 103(a) over Stewart et al. in view of U.S. Patent No. 6,813,503 ("Zillikens et al.").

ARGUMENT

I. LEGAL STANDARDS

A. ANTICIPATION UNDER 35 U.S.C. § 102(b)

Some claims have been rejected under 35 U.S.C. § 102(b) as anticipated. The legal standards for anticipation under 35 U.S.C. §102 are well-settled. The "basic test" for anticipation of a patent claim by a prior art reference is this: to establish anticipation, there must be "identity of invention: the claimed invention, as described in appropriately construed claims, must be the same as that of the reference." Glaverbel S.A. v. Northlake Mktg. & Supply, Inc., 45 F.3d 1550, 1554, 33 U.S.P.Q.2d 1496, 1498 (Fed. Cir. 1995); see also Cont'l Can Co. v. Monsanto Co., 948 F.2d 1264, 1267, 20 U.S.P.Q.2d 1746, 1748 (Fed. Cir. 1991). "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." Manual of Patent

Examining Procedure (MPEP), § 2131 (quoting Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631, 2 U.S.P.Q.2d 1051, 1053 (Fed. Cir. 1987)).

B. OBVIOUSNESS UNDER 35 U.S.C. § 103(a)

Some claims have been rejected under 35 U.S.C. §103(a) as obvious. The legal standards under 35 U.S.C. § 103(a) are also well-settled. Obviousness under 35 U.S.C. § 103(a) is a legal conclusion involving four factual inquiries:

(1) the scope and content of the prior art;

(2) the differences between the claims and the prior art;

(3) the level of ordinary skill in the pertinent art; and

(4) secondary considerations, if any, of non-obviousness.

MPEP § 2141. See also Graham v. John Deere Co., 383 U.S. 1, 148 U.S.P.Q. 459 (1966).

In proceedings before the Patent and Trademark Office (PTO), the Examiner bears the burden of establishing a prima facie case of obviousness based upon the prior art. In re Piasecki, 745 F.2d 1468, 1471-72, 223 U.S.P.Q. 785, 787-88 (Fed. Cir. 1984). A prima facie case of obviousness requires that the prior art reference or references teaches or suggests all of the claimed limitations. In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974); MPEP §§ 2142, 2143.03. "The Examiner can satisfy this burden only by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the references." In re Fritch, 972 F.2d 1260, 1265, 23 U.S.P.Q.2d 1780, 1783 (Fed. Cir. 1992); In re Fine, 837 F.2d 1071, 1074, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988); In re Lalu, 747 F.2d 703, 705, 223 U.S.P.Q. 1257, 1258 (Fed. Cir. 1984); Ashland Oil, Inc. v. Delta Resins & Refractories, Inc., 776 F.2d 281, 297 n.24, 227 U.S.P.Q. 657, 667 n.24 (Fed. Cir. 1985); ACS Hosp. Sys., Inc. v. Montefiore Hosp., 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984).

When a reference teaches away from the claimed invention, that teaching is strong evidence of non-obviousness. See United States v. Adams, 383 U.S. 39, 148 U.S.P.Q. 79 (1966); In re Royka, 490 F.2d 981, 180 U.S.P.Q. 580 (CCPA 1974).

As noted by the Federal Circuit, the "factual inquiry whether to combine references must be thorough and searching." McGinley v. Franklin Sports, Inc., 262 F.3d 1339, 1351-52, 60 U.S.P.Q.2d 1001, 1008 (Fed. Cir. 2001). Further, it "must be based on objective evidence of record." In re Lee, 277 F.3d 1338, 1343, 61 U.S.P.Q.2d 1430, 1433 (Fed. Cir. 2002). The teaching or suggestion to make the claimed combination must be found in the prior art, and not in the appellant's disclosure. In re Vaeck, 947 F.2d 488, 20 U.S.P.Q.2d 1438 (Fed. Cir. 1991). The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. In re Mills, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). "It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to '[use] that which the inventor taught against its teacher.'" Lee at 1344, 61 U.S.P.Q.2d at 1434 (citing W.L. Gore and Assoc. v. Garlock, Inc., 721 F.2d 1540, 1553, 220 U.S.P.Q. 303, 312-13 (Fed. Cir. 1983)). In KSR Intl'. v. Teleflex, Inc., No. 04-1350 (U.S. Apr. 30, 2007), the U.S. Supreme Court rejected a rigid and mandatory application of the teaching, suggestion, or motivation test, instead recognizing the test as a "helpful insight." Id. at 15. The Court said, "Often it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed." Id. at 14.

II. REJECTION OF CLAIMS 1-5, 7-9, 11-13, 15-16, 18-21, 23-24, 27-28, 30-36, 38-41, 43-44, AND 46-48 UNDER 35 U.S.C. § 102(B) AS BEING ANTICIPATED BY U.S. PATENT NO. 6,970,927 ("STEWART ET AL.")

In section 7 of the final Office Action, claims 1-5, 7-9, 11-13, 15, 16, 18-21, 23, 24, 27, 28, 30-36, 38-41, 43, 44, 46-48, and 50-53 were rejected under 35 U.S.C. § 102(b) as being anticipated by Stewart et al. (U.S. Patent No. 6,970,927). Appellants respectfully request reconsideration of the rejection in view of the reasons that follow.

A. Claims 1-5, 7-9, 11-13, 15, 16, and 50

Claim 1 is in independent form and recites a combination including, among other elements, "selecting a single level of security from a group of more than two security levels . . . wherein the group of more than two security levels is defined by a user of the network user node," which is not disclosed by Stewart et al.

In making the rejection of independent claim 1, the Examiner stated in the final Office Action that Stewart et al. discloses:

> wherein the group of more than two security levels is defined by a user of the network user node (Col 3, lines 15-28; Col 8, lines 44-50; Col. 10, line 65 to Col 11, lines 3; the access information may be provided by the PCD of the user; plurality of the systems such as AP, MIB, or PCD with memory to support/manage the access features; using PCD instead of access point/MIB).

Appellants respectfully disagree with the Examiner's conclusion. Specifically, Appellants submit that Stewart et al. does not disclose, either expressly or inherently, security levels "defined by a user of the network user node." The various portions of Stewart et al. cited by the Examiner in the final Office Action may disclose that "the access information may be provided by the PCD of the user," (col. 3, lines 22-24), that a "[personal computing device] 110 . . . may include a memory medium on which computer programs or data according to the present invention may be stored," (col. 8, lines 45-49), and that a "user may configure the System ID on his/her [personal computing device] to uniquely identify the network provider to which the user has selected or subscribed," (col. 10, line 67 to col. 11,

line 2). However, the cited portions of Stewart et al. do not disclose security levels "defined by a user of [a] network user node," as recited in independent claim 1. Appellants submit that, in rejecting claim 1, the Examiner seems to be equating security levels that are defined by a user of a computing device (as in claim 1) and access levels that may be stored on a computing device of a user (as in Stewart et al.), which is improper. These are two very different concepts. For example, in Stewart et al., a user is granted a particular level of network access based upon, for example, the location of the user. However, Stewart et al. does not teach or suggest that the user defines a particular level of network access (much less a security level for a computing device). Accordingly, Appellants submit that the Examiner has mischaracterized Stewart et al. in rejecting independent claim 1.

In the Advisory Action, the Examiner further cited column 20, lines 25-29 of Stewart et al. for additional support for the rejection of claim 1. Appellants submit that the additional portions of Stewart et al. cited in the Advisory Action do not make up for the deficiencies of the final Office Action, in that the Examiner has still failed to show that Stewart et al. discloses security levels "defined by a user of [a] network user node," as recited in independent claim 1. For example, Stewart et al. may disclose that a "first access point" receives "identification information from a portable computing device," and that the identification information may "indicate[] an access level" (col. 19, line 65 to col. 20, line 1). Further, Stewart et al. may disclose that the "access level" may be a "first access level" or a "second access level," and that the "access level" may be "stored in the memory of the personal computing device" (col. 20, lines 24-59). However, as discussed above with respect to the cited portions of the final Office Action, Stewart et al. does not disclose the subject matter of claim 1. Appellants have found no portion(s) of Stewart et al., cited by the Examiner or otherwise, that disclose "selecting a single level of security from a group of more than two security levels . . . wherein the group of more than two security levels is defined by a user of the network user node," as recited in independent claim 1.

Appellants further submit that this limitation is not inherent in Stewart et al., because the limitation is not "necessarily present in the thing described in the reference," (MPEP § 2112(IV)), as is required under the principle of inherency. For example, in Stewart et al., the access information may be associated with a network provider and stored on a personal computing device. In such a case, the access levels are not defined by a user of the personal computing device, but are merely stored on the device. Appellants again submit that, in rejecting claim 1, the Examiner seems to be equating security levels that are defined by a user of a computing device (as in claim 1) and access levels that may be stored on a computing device of a user (as in Stewart et al.).

Accordingly, because Stewart et al. fails to disclose at least one limitation of independent claim 1, Appellants respectfully request that the rejection of independent claim 1, and corresponding dependent claims 2-5, 7-9, 11-13, 15, 16, and 50, be withdrawn.

B. Claim 12

Claim 12 depends from claim 1, and as discussed above, is believed to be patentable for at least the same reasons that independent claim 1 is patentable. Claim 12 is believed to be further patentable over Stewart et al. because Stewart et al. fails to teach or suggest at least one additional limitation of claim 12.

Claim 12 recites "wherein the security levels are provided by the user of the network user node for a variety of locations" which is not disclosed by Stewart et al. As discussed above with respect to independent claim 1, Stewart et al. does not disclose security modifications that are defined, or provided, by a user of the network user node, and more specifically, Stewart et al. does not disclose security modifications that are provided by the user of the network user node for a variety of locations. Appellants submit that in rejecting claim 12, the Examiner again seems to be equating security levels that are provided by a user of a computing device (as in claim 12) and access levels that may be stored on a computing device of a user (as in Stewart et al.). Accordingly, Appellants respectfully request that the rejection of dependent claim 12 be withdrawn.

C. Claim 15

Claim 15 depends from claim 1, and as discussed above, is believed to be patentable for at least the same reasons that independent claim 1 is patentable. Claim 15 is believed to be further patentable over Stewart et al. because Stewart et al. fails to teach or suggest at least one additional limitation of claim 15.

Claim 15 recites "wherein the step of modifying the security protection for the network user node includes a complete denial of access to information using the network user node," which is not disclosed by Stewart et al. Stewart et al. is directed to "a network infrastructure to support multiple access levels for users of a wired or wireless network system." Col. 1, lines 23-26. Stewart et el. does not address the more general case of "access to information using [a] network user node" recited in claim 15, which may or may not include network access. For example, in ¶ 0035 of the present application, Appellants recite:

> The security level setting could include restrictions or complete blocks on access to either network user node 110 as a whole, information stored on network user node 110, or any subset of information stored on the network user node 110. The security settings could also include restrictions or blocks on access to information available on a remote system accessible using network user node 110 over wireless network 120.

Appellants submit that providing different access levels to networks (as in Stewart et al.) is a very different concept from Appellants claimed invention, where security levels may provide complete blocks on information stored on a network user node. Accordingly, because Stewart et al. fails to disclose at least one additional limitation in dependent claim 15, Appellants respectfully request that the rejection of dependent claim 15 be withdrawn.

D. Claims 18, 20, 21, 23, 24, 27, 28, and 51

Claim 18 is in independent form and recites a combination including, among other elements, "a storage device for storing a table of security modifications . . . , the security modifications being defined by a user of the network user node," which is not disclosed by Stewart et al. The Examiner stated on page 4 of the final Office Action that "[claim 18] is rejected applying the above rejection of claim 1." Referring to Section II.A. above, Appellants submit that independent claim 18 is patentable for at least the same reasons claim 1 is patentable, in that Stewart et al. fails to disclose at least one limitation of claim 18. Therefore, because Stewart et al. fails to disclose at least one limitation of independent claim 18, Appellants respectfully request that the rejection of independent claim 18, and corresponding dependent claims 20, 21, 23, 24, 27, 28, and 51, be withdrawn.

E. Claims 30-36, and 52

Claim 30 is in independent form and recites a combination including, among other elements, "wherein the group of more than two levels are defined by a user of the network user node," which is not disclosed by Stewart et al. Claim 30 recites a similar limitation to that contained in claims 1 and 18 which, as discussed above, are believed to be patentable over Stewart et al. Referring to Section II.A. above, Appellants submit that claim 30 is patentable for at least the same reasons that claims 1 and 18 are patentable. Accordingly, Appellants respectfully request that the rejection of independent claim 30, and corresponding dependent claims 31-36 and 52, be withdrawn.

F. Claims 38-41, 43, 44, 46-48 and 53

Claim 38 is in independent form and recites a combination including, among other elements, "a network user node . . . wherein the network user node performs security modifications based on the physical location of the network user node," which is not disclosed by Stewart et al.

In making the rejection of independent claim 38, the Examiner stated in the final Office Action that Stewart et al. discloses

> wherein the network user node performs security modifications based on the physical location of the network user node (Col 8, lines 26-42; provide services to the user based on the geographic location information; Col 19, lines 60-67; Col 20, lines 1-10; access level is determined based on geographic location).

Appellants submit that none of the cited portions of Stewart et al. disclose "a network user node . . . wherein the network user node performs security modifications based on the physical location of the network user node," as recited in independent claim 38. More specifically, Appellants have found no portion(s) of Stewart et al., cited by the Examiner or otherwise, that disclose a system where "the network user node performs security modifications." Rather, in Stewart et al., access levels are determined by the wireless network system (or components thereof), which may receive the access level information from a personal computing device. For example, referring to FIG. 2 (which illustrates a portion of a wireless network system) and col. 9, lines 42-61 of Stewart et al., "one or more access controllers, e.g., computer systems configured to determine or control network service access, may be provided . . . to verify user or subscriber access." In Stewart et al., the personal computing device does not perform security modifications. Therefore, because Stewart et al. does not disclose at least one limitation of independent claim 38, Appellants respectfully request that the rejection of independent claim 38, and corresponding dependent claims 39-41, 43, 44, 46-48, and 53, be withdrawn.

G. Claim 46

Claim 46 depends from independent claim 38, and as discussed above, is believed to be patentable for at least the same reasons that independent claim 38 is patentable. Claim 46 is believed to be further patentable over Stewart et al. because Stewart et al. fails to teach or suggest at least one additional limitation of claim 46.

Claim 46 recites "wherein the table stored on the storage device includes user defined protection settings based on at least one physical location," which is not disclosed by Stewart et al. As discussed above with respect to independent claim 1, Stewart et al. does not disclose protection settings that are defined, or provided, by a user of the network user node, and more specifically, Stewart et al. does not disclose "user defined protection settings based on at least one physical location." Appellants submit that in rejecting claim 46, the Examiner seems to be equating protection settings that are "user defined" (as in claim 46) and access levels that may be stored on a computing device of a user (as in Stewart et al.). Accordingly, Appellants respectfully request that the rejection of dependent claim 46 be withdrawn.

III. REJECTION OF CLAIMS 6, 10, 14, 22, 25, 37, 42, AND 45 UNDER 35 U.S.C. § 103(A) AS BEING UNPATENTABLE OVER STEWART ET AL. IN VIEW OF U.S. PATENT APPL. PUBL. NO. 2002/0138632 ("BADE ET AL.").

In section 7 of the final Office Action, claims 6, 10, 14, 22, 25, 37, 42, and 45 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Stewart et al. in view of Bade et al. (U.S. Patent Appl. Publ. No. 2002/0138632).

A. Claims 6, 10, 14, 22, 25, 37, 42, and 45

Claims 6, 10, 14, 22, 25, 37, 42, and 45 depend from independent claims 1, 18, 30, and 38, respectively. As discussed above, independent claims 1, 18, 30, and 38 are believed to be patentable over Stewart et al. Bade et al. does not make up for the deficiencies of Stewart et al. with respect to independent claims 1, 18, 30, and 38. Bade et al. is directed to "a system and method for providing positional authentication for client server systems." (¶ 0002). Bade et al. does not teach or suggest "selecting a single level of security from a group of more than two security levels . . . wherein the group of more than two security levels is defined by a user of the network user node," as recited in independent claim 1, nor does Bade et al. teach or suggest the similar limitations recited in each of independent claims 18, 30, and 38. Accordingly, Appellants submit that independent claims 1, 18, 30, and 38, and corresponding dependent claims 6, 10, 14, 22, 25, 37, 42, and 45, are patentable over Stewart et al. in view of Bade et al., and respectfully request that the rejection be withdrawn.

B. Claims 25, 37, and 45

Appellants believe that dependent claims 25, 37, and 45 are further patentable over the combination of Stewart et al. and Bade et al. because the cited references also fail to teach or suggest the limitation of "wherein the WLAN protocol includes the Bluetooth wireless network protocol," as recited in each of dependent claims 25, 37, and 45.

In support of the rejection, the Examiner stated in the final Office Action that

> Bade et al's teaching of "3D triangulation" and "GPS system" implies use of Bluetooth or any suitable/popular wireless network protocol for that purpose.

Appellants respectfully disagree with the Examiner. Bade et al. is directed to "a system and method for providing positional authentication for client-server systems." (¶0002.) In Bade et al., a "host server 106 includes an authentication module 216 that is configured to receive data from [a] remote client 104 [and control and authenticate] access rights to the host server 106." (¶ 00230. Appellants submit that the "3D triangulation" and "GPS system" of Bade et al. do not "imply," as indicated by the Examiner, the use of a Bluetooth wireless network protocol as in the rejected claims.

For example, in dependent claim 25 (which depends from claim 18), the Bluetooth wireless network protocol is used by "a communication device capable of transmitting a data signal to the network user node containing instructions to modify the security protection for the node." The portions of Bade et al. cited by the Examiner are directed to "positional access systems" that may utilize GPS or triangulation technology. (¶ 0023). Appellants submit that this disclosure does not teach or suggest transmitting instructions to modify security protection for a network user node, as in claim 25. Rather, Bade et al. suggests only methods or systems (e.g., (3D) triangulation, GPS) that may be used to determine location. The Examiner has not cited, nor have Appellants found in reviewing the disclosures of Stewart et al. and Bade et al., any teaching or suggestion of the use of a Bluetooth wireless network protocol. Thus, Appellants submit that Stewart et al. in view of Bade et al. fails to teach or suggest at least one additional limitation in dependent claim 25, and that claim 25 is

patentable over the cited references. Claims 37 and 45 contain similar limitations to claim 25, and are believed to be patentable for at least the same reasons.

Accordingly, because the combination of Stewart et al. and Bade et al. fails to teach or suggest "wherein the WLAN protocol includes the Bluetooth wireless network protocol," as recited in each of dependent claims 25, 37, and 45, Appellants respectfully request that the rejection be withdrawn.

IV. REJECTION OF CLAIMS 17, 29, AND 49 UNDER 35 U.S.C. § 103(A) AS BEING UNPATENTABLE OVER STEWART ET AL. IN VIEW OF U.S. PATENT NO. 6,813,503 ("ZILLIKENS ET AL.").

In section 8 of the final Office Action, claims 17, 29, and 49 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Stewart et al. in view of Zillikens et al. (U.S. Patent No. 6,813,503).

A. Claims 17, 29, and 49

Claim 17 depends from independent claim 1. Claim 29 depends from independent claim 18. Claim 49 depends from independent claim 38. As discussed above, claims 1, 18, and 38 are believed to be patentable over Stewart et al. Zillikens et al. does not make up for the deficiencies of Stewart et al. with respect to independent claim 1. Accordingly, Appellants submit that independent claims 1, 18, and 38, and corresponding dependent claims 17, 29, and 49, are patentable over Stewart et al. in view of Zillikens et al., and respectfully request that the rejection be withdrawn.

V. CONCLUSION

In view of the foregoing, Appellants respectfully request that the Board reverse all of the claim rejections and indicate that a Notice of Allowance respecting all of the claims presented in this appeal be issued.

Respectfully submitted,

Date 5/29/2007

By _____

FOLEY & LARDNER LLP
Customer Number: 26371
Telephone: (414) 319-7306
Facsimile: (414) 297-4900

Matthew J. Swietlik
Attorney for the Appellants
Registration No. 58,428

CLAIMS APPENDIX

1. A method of adjusting security for a network user node in communication with a network based upon the location of the node, comprising:

determining the location of a network user node;

selecting a single level of security from a group of more than two security levels based on the determined location, the group of more than two security levels being stored in the memory of the network user node; and

modifying the security protection for the network user node based upon the selected level of security;

wherein the group of more than two security levels is defined by a user of the network user node.

2. The method of claim 1, wherein the network user node is a mobile computing device having a display.

3. The method of claim 1, wherein the network user node's location is determined using a location sensing system.

4. The method of claim 3, wherein the location sensing system is a global positioning satellite (GPS) system.

5. The method of claim 3, wherein the location sensing system uses nearby access points to determine location.

6. The method of claim 3, wherein the location sensing system uses signal bouncing and triangulation to determine network user node location.

7. The method of claim 3 wherein the network user node is in direct communication with the location sensing system.

8. The method of claim 1, wherein the step of sending a data signal includes transmitting the data signal using a wireless local area network (WLAN) protocol.

9. The method of claim 8, wherein the WLAN protocol includes the IEEE 802.11 protocol.

10. The method of claim 8, wherein the WLAN protocol includes the Bluetooth wireless network protocol.

11. The method of claim 1, wherein the selecting step is carried out by reference to a table of desired security modifications based upon the location of the network user node.

12. The method of claim 11, wherein the security levels are provided by the user of the network user node for a variety of locations.

13. The method of claim 11, wherein the selected security level is based on the type of location determined for the network user node.

14. The method of claim 1, wherein the step of modifying the security protection for the network user node includes restricting access to information unless a password is properly entered.

15. The method of claim 1, wherein the step of modifying the security protection for the network user node includes a complete denial of access to information using the network user node.

16. The method of claim 1, wherein the step of modifying the security protection for the network user node includes a denial to a subset of the information accessible using the node.

17. The method of claim 1, wherein the step of modifying the security protection for the network user node includes modifying data encryption parameters to change the strength of encryption on data transmitted by the network user node.

18. A computer system for modifying security settings for a network user node based on the location of the node comprising:

an input device having a communicative coupling with a system for determining the location of a network user node;

a storage device for storing a table of security modifications to be performed based on a plurality of locations for the network user node, the security modifications including more than two levels, the security modifications being defined by a user of the network user node;

a processor coupled to a storage device for processing information, storing on a storage device, and generating a security modification instruction; and

a communication device capable of transmitting a data signal to the network user node containing instructions to modify the security protection for the node.

19. The system of claim 18, wherein the network user node is a mobile computing device having a display.

20. The system of claim 18, wherein the system for determining the location of a network user node accesses and interprets global positioning satellite (GPS) signals.

21. The system of claim 18, wherein the system for determining the location of a network user node uses nearby access points to determine the location.

22. The system of claim 18, wherein the system for determining the location of a network user node uses signal bouncing and triangulation to determine location.

23. The system of claim 18, wherein the communication device transmits the data signal using a wireless local area network (WLAN) protocol.

24. The system of claim 23, wherein the WLAN protocol includes the IEEE 802.11 protocol.

25. The system of claim 23, wherein the WLAN protocol includes the Bluetooth wireless network protocol.

26. (Canceled).

27. The system of claim 18, wherein the table stored on the storage device includes security levels customized based upon the type of location received from the system providing the location of the network user node.

28. The system of claim 18, wherein the system sends a signal modifying information access restrictions on the network user node.

29. The system of claim 18, wherein the system sends a signal modifying the data encryption parameters to change the strength of encryption on data transmitted by the network user node.

30. A method of adjusting security for a network user node having a processor, a memory coupled to the processor, a wireless transceiver, and a physical location determining device in communication with a network based upon the physical location of the node, comprising:

receiving physical location information using a network user node; and

using a network user node to modify security protection for data to a single level from a group of more than two levels, based upon the physical location information;

wherein the group of more than two levels are defined by a user of the network user node.

31. The method of claim 30, wherein the network user node is a mobile computing device having a display.

32. The method of claim 30, wherein the network user node is used to access a table of security levels and physical location associations.

33. The method of claim 32, wherein the table of security levels are stored in the memory of the network user node.

34. The method of claim 30, wherein the network user node encrypts data based on the selected security level.

35. The method of claim 30, wherein the network user node sends and receives data over a wireless local area network (WLAN).

36. The method of claim 35, wherein the WLAN protocol includes the IEEE 802.11 protocol.

37. The method of claim 35, where the WLAN protocol includes the Bluetooth wireless network protocol.

38. A system implemented on a network user node for modifying security settings based on the physical location of the node comprising:

a system for determining the physical location of the network user node coupled to the network user node;

a processor for processing information, storing information on a storage device, and accessing a table of security modification instructions, the table including more than two unique security modifications; and

a storage device coupled to the network user node for storing a table of security modifications;

wherein the network user node performs security modifications based on the physical location of the network user node.

39. The system of claim 38, wherein the network user node is a mobile computing device having a display.

40. The system of claim 38, wherein the system for determining the physical location of the network user node accesses and interprets global positioning satellite (GPS) signals.

41. The system of claim 38, wherein the system for determining the physical location of the network user node uses nearby access points to determine location.

42. The system of claim 38, wherein the system for determining the physical location of the network user node uses signal bouncing and triangulation to determine location.

43. The system of claim 38, wherein the network user node can transmit and receive data signals using a wireless local area network (WLAN) protocol.

44. The system of claim 43, wherein the WLAN protocol includes the IEEE 802.11 protocol.

45. The system of claim 43, wherein the WLAN protocol includes the Bluetooth wireless network protocol.

46. The system of claim 38, wherein the table stored on the storage device includes user defined protection settings based on at least one physical location.

47. The system of claim 38, wherein the table stored on the storage device includes protection settings customized based upon the type of location of the network user node.

48. The system of claim 38, wherein the network user node system modifies information access restrictions based upon a security modification associated with the physical location of the network user node.

49. The system of claim 38, wherein the network user node modifies the data encryption parameters to change the strength of encryption on data based on a security modification associated with the physical location of the network user node.

50. The method of claim 1, wherein the network user node is a portable handheld device.

51. The system of claim 18, wherein the network user node is a portable handheld device.

52. The method of claim 30, wherein the network user node is a portable handheld device.

53. The system of claim 38, wherein the network user node is a portable handheld device.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.